PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-222172

(43)Date of publication of application : 09.08.2002

(51)Int.Cl. G06F 15/00
G06F 13/00
H04L 9/32

(21)Application number : 2001-017207

(22)Date of filing : 25.01.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

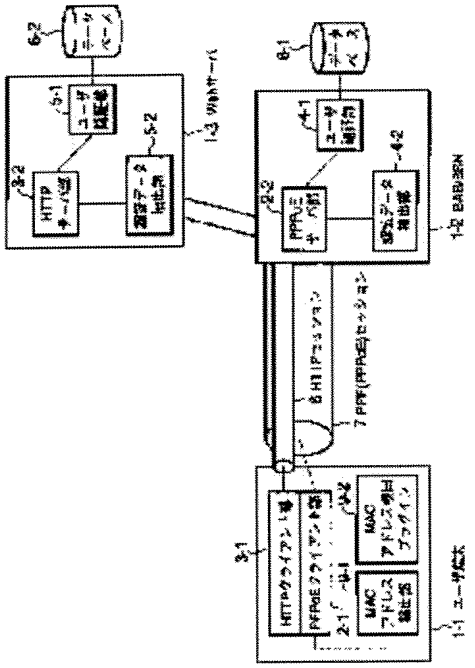
(72)Inventor : NAKAGAWA KOICHI
IRIE KAZUNARI
SASAKI MASAHITO
WATASE JUNPEI

(54) METHOD FOR USER AUTHENTICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To enhance security by using also an MAC address as an authentication parameter.

SOLUTION: A user name, a password and the MAC address are transmitted, when connection is requested, from a PPPoE client part 2-1 of a user terminal 1-1 having an MAC address detecting part 9-1 to a center side as a portion of an internal data of a PPP frame in a PPPoE frame, the user name, the password and the MAC address are extracted in the center side having a PPPoE sever 2-2 from the internal data of the PPP frame in the PPPoE frame, the extracted user name, password and MAC address are collated with an authentication database, and the connection is allowed only when the both are consistent each other.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号
特開2002－222172
（P2002－222172A）
(43)公開日　平成14年８月９日(2002.8.9)

(51)Int.Cl.[7]		識別記号	FI		テーマコード*(参考)	
G06F	15/00	330	G06F	15/00	330C	5B085
	13/00	510		13/00	510A	5J104
H04L	9/32		H04L	9/00	673A	

審査請求 有　請求項の数2 ＯＬ （全 7 頁）

(21)出願番号　特願2001－17207(P2001－17207)

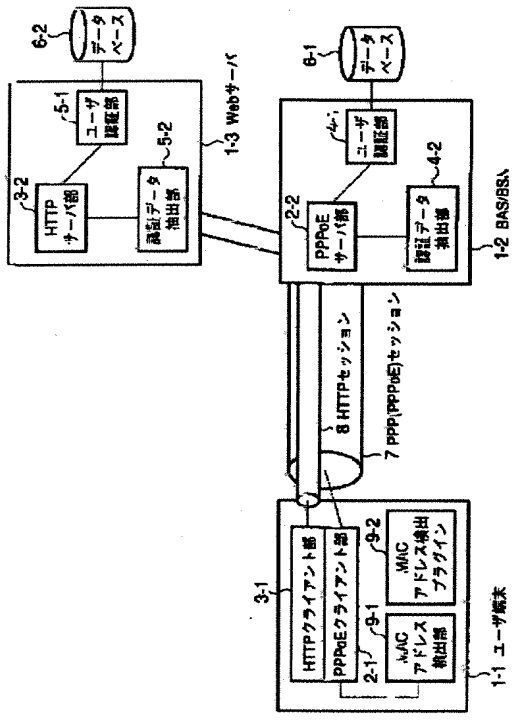
(22)出願日　平成13年１月25日(2001.1.25)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　中川　広一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　入江　一成
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100058479
弁理士　鈴江　武彦　（外２名）

最終頁に続く

(54)【発明の名称】　ユーザ認証方法

(57)【要約】
【課題】本発明の課題は、ＭＡＣアドレスも認証パラメータとして用いることにより、セキュリティーの高いユーザ認証方法を提供することにある。
【解決手段】本発明は、ＭＡＣアドレス検出部９－１を有するユーザ端末１－１のＰＰＰｏＥクライアント部２－１から、接続要求時にユーザ名とパスワードとＭＡＣアドレスをＰＰＰｏＥフレーム内のＰＰＰフレームの内部データの一部としてセンタ側へ送出し、ＰＰＰｏＥサーバ部２－２を有するセンタ側で、ＰＰＰｏＥ内のＰＰＰフレームの内部データからユーザ名とパスワードとＭＡＣアドレスを抽出し、抽出されたユーザ名とパスワードとＭＡＣアドレスを認証データベースと照合し、一致した場合にのみ接続を許可することを特徴とする。



【特許請求の範囲】
【請求項１】　ＭＡＣアドレスを検出するＭＡＣアドレス検出部を有する端末側のＰＰＰｏＥクライアント部から、接続要求時にユーザ名とパスワードとＭＡＣアドレスをＰＰＰｏＥフレーム内のＰＰＰフレームの内部データの一部としてセンタ側へ送出するステップと、
ＰＰＰｏＥサーバ部を有するセンタ側で、ＰＰＰｏＥ内のＰＰＰフレームの内部データからユーザ名とパスワードとＭＡＣアドレスを抽出するステップと、
前記ステップで抽出されたユーザ名とパスワードとＭＡＣアドレスを認証データベースと照合し、一致した場合にのみ接続を許可するステップとを有することを特徴とするユーザ認証方法。
【請求項２】　ＭＡＣアドレスを検出するＭＡＣアドレス検出部を有する端末側のＨＴＴＰクライアント部から、Ｗｅｂサイトへの接続要求時にユーザ名とパスワードとＭＡＣアドレスをＨＴＴＰフレームの内部データの一部としてセンタ側へ送出するステップと、
ＨＴＴＰサーバ部を有するセンタ側で、ＨＴＴＰフレームの内部データからユーザ名とパスワードとＭＡＣアドレスを抽出するステップと、
前記ステップで抽出されたユーザ名とパスワードとＭＡＣアドレスを認証データベースと照合し、一致した場合にのみ接続を許可するステップとを有することを特徴とするユーザ認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信回線を介してユーザ端末（パソコン）とネットワークサイドのサーバ（コンピュータ）間の通信を行うコンピュータ通信システムにおいて、セキュリティの高いウェブ（Ｗｅｂ）アクセスやコンテンツダウンロードを提供するためのＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスを用いたユーザ認証方法に関するものである。
【０００２】
【従来の技術】これまで通信回線を介してコンピュータ間の通信を行うための様々なシステムが開発されている。コンピュータ通信のうち、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）プロトコルを用いるものはインターネットあるいはエキストラネットとして広く普及してきた。通信インフラとしては、電話回線を利用したダイヤルアップによるモデム通信、ＣＡＴＶ回線に接続されたモデムにより通信を行うケーブルモデムシステム、無線回線あるいは光ファイバを利用したシステムが開発されている。近年特に、従来からのメタリック電話回線を共用してデータ通信が可能なＡＤＳＬ（Ａｓｙｍｍｅｔｒｉｃ　Ｄｉｇｉｔａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｌｏｏｐ）が注目されている。これはユーザ側にＡＴＵと呼ばれるＡＤＳＬ終端装置、センタ側にはＤＳＬＡＭ（ＡＤＳＬ　Ａｃｃｅｓｓ　Ｍｕｌｔｉｐｌｅｘｅｒ）と呼ばれる装置を設置し、さらにその先にＢＡＳ（Ｂｒｏａｄｂａｎｄ　Ａｃｃｅｓｓ　Ｓｅｒｖｅｒ）あるいはＢＳＮ（Ｂｒｏａｄｂａｎｄ　Ｓｅｒｖｉｃｅ　Ｎｏｄｅ）と呼ばれるノード装置を設置し、ユーザを収容する。
【０００３】現在、ＡＤＳＬではＩＰ通信を行うために、ユーザ端末からＢＡＳまでをブリッジモードで接続し、イーサネット（登録商標）（Ｅｔｈｅｒｎｅｔ（登録商標））上でＰＰＰ（Ｐｏｉｎｔ－ｔｏ－Ｐｏｉｎｔ　Ｐｒｏｔｏｃｏｌ）を用いる、ＰＰＰｏＥ（ＰＰＰ　ｏｖｅｒ　Ｅｔｈｅｒｎｅｔ）が利用されている。一般的にＰＰＰでは、ユーザ名、パスワードを用いて、認証を行っている。しかし、他人にユーザ名とパスワードが漏洩した場合は、本人でなくとも接続が可能となり、ユーザ名とパスワードのみの認証では、本人であることの確認が不十分である。
【０００４】また、同様に、インターネット普及のキラーアプリケーションとなったＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）における認証においても一般的にユーザ名とパスワードによってサイトへの接続認証が行われている。この場合も、他人にユーザ名とパスワードが漏洩することで、本人でなくとも当該サイトに接続が可能となる。
【０００５】このようにユーザ名とパスワードのみによる認証は他人によるなりすましを防ぐことができないと言う問題があった。
【０００６】従来のＰＰＰ接続におけるユーザ認証方法の１例を図６及び図７に示す。図６は一般的なユーザ認証システム構成図であり、図７は図６のユーザ認証システムにおける処理フロー示している。図中、１－１はユーザ端末、１－２はＢＡＳあるいはＢＳＮ、１－３はＷｅｂサーバ、２－１はＰＰＰｏＥクライアント部、２－２はＰＰＰｏＥサーバ部、３－１はＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）クライアント部、３－２はＨＴＴＰサーバ部、４－１はＰＰＰにおけるユーザ認証部、５－１はＨＴＴＰにおけるユーザ認証部、６－１，６－２は認証データベース、７はＰＰＰ（ＰＰＰｏＥ）セッション、８はＨＴＴＰセッションを示す。また図示しないが、ユーザ端末１－１とＢＡＳ１－２のあいだにＡＴＵとＤＳＬＡＭが設置される。ユーザ端末１－１とＡＴＵはＥｔｈｅｒｎｅｔ接続、ＡＴＵとＤＳＬＡＭはＡＤＳＬ回線接続、ＤＳＬＡＭとＢＡＳ１－２はＡＴＭ専用線による接続が一般的である。
【０００７】ユーザ端末１－１がＷｅｂサーバ１－３へアクセスするために、ＰＰＰｏＥクライアント部２－１が起動し、ＰＰＰｏＥクライアント部２－１とＰＰＰｏＥサーバ部２－２との間でＰＰＰセッション７を確立しようとする。そのために、ユーザは「ユーザ＠Ｒｅａｌｍ名」と「パスワード」を入力し、ＢＡＳ１－２内のユ

ーザ認証部４－１にデータを渡し、認証データベース６－１と照合を行い認証を行う。ユーザデータが正しければ、ＰＰＰ（ＰＰＰｏＥ）セッション７を確立する。その後、ＨＴＴＰクライアント部３－１はＨＴＴＰサーバ部３－２との間で通信を行う。この場合、認証の必要なＨＴＴＰサーバ３－２へ接続するために、ＨＴＴＰクライアント部３－１から入力されたユーザ名、パスワードをユーザ認証部５－１で認証データベース６－２と照合して認証を行う。

【０００８】このようにユーザ名とパスワードのみで認証するのが一般的である。そのため、ユーザ名、パスワードの漏洩によって、他人によるなりすましが起こるという問題があった。

【０００９】

【発明が解決しようとする課題】上記のように従来の技術を用いた方式では、ＰＰＰ（ＰＰＰｏＥ）セッションを確立する際と認証が必要なＨＴＴＰサーバ部へ接続する際において、ユーザ名とパスワードのみで認証を行うため、接続してくるユーザが本人であるか確認することができず、なりすましが可能であった。

【００１０】本発明は上記の事情に鑑みてなされたもので、ＰＰＰ（ＰＰＰｏＥ）でセッションを確立し、そのセッション上でＨＴＴＰプロトコルによってデータの送受信を行う通信において、ＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）ごとに一意であるＭＡＣアドレスも認証パラメータとして用いることにより、セキュリティーの高いユーザ認証方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成するために本発明のユーザ認証方法は、ＭＡＣアドレスを検出するＭＡＣアドレス検出部を有する端末側のＰＰＰｏＥクライアント部から、接続要求時にユーザ名とパスワードとＭＡＣアドレスをＰＰＰｏＥフレーム内のＰＰＰフレームの内部データの一部としてセンタ側へ送出するステップと、ＰＰＰｏＥサーバ部を有するセンタ側で、ＰＰＰｏＥ内のＰＰＰフレームの内部データからユーザ名とパスワードとＭＡＣアドレスを抽出するステップと、前記ステップで抽出されたユーザ名とパスワードとＭＡＣアドレスを認証データベースと照合し、一致した場合にのみ接続を許可するステップとを有することを特徴とする。

【００１２】また本発明のユーザ認証方法は、ＭＡＣアドレスを検出するＭＡＣアドレス検出部を有する端末側のＨＴＴＰクライアント部から、Ｗｅｂサイトへの接続要求時にユーザ名とパスワードとＭＡＣアドレスをＨＴＴＰフレームの内部データの一部としてセンタ側へ送出するステップと、ＨＴＴＰサーバ部を有するセンタ側で、ＨＴＴＰフレームの内部データからユーザ名とパスワードとＭＡＣアドレスを抽出するステップと、前記ステップで抽出されたユーザ名とパスワードとＭＡＣアドレスを認証データベースと照合し、一致した場合にのみ接続を許可するステップとを有することを特徴とする。

【００１３】

【発明の実施の形態】以下図面を参照して本発明の実施形態例を詳細に説明する。

【００１４】図１は本発明の実施形態例を示すシステム構成図、図２は本発明の実施形態例に係るＰＰＰｏＥにおける認証機能のレイヤ構成図、図３は本発明の実施形態例に係るＰＰＰｏＥにおける認証の処理フローを示すシーケンス図、図４は本発明の実施形態例に係るＨＴＴＰにおける認証機能のレイヤ構成図、図５は本発明の実施形態例に係るＨＴＴＰにおける認証の処理フローを示すシーケンス図である。

【００１５】図中、１－１はユーザ端末、１－２はＢＡＳあるいはＢＳＮ、１－３はＷｅｂサーバ、２－１はＰＰＰｏＥクライアント部、２－２はＰＰＰｏＥサーバ部、３－１はＨＴＴＰクライアント部、３－２はＨＴＴＰサーバ部、４－１はＰＰＰにおけるユーザ認証部、４－２はＰＰＰｏＥサーバ部における認証データ抽出部、５－１はＨＴＴＰにおけるユーザ認証部、５－２はＨＴＴＰサーバ部における認証データ抽出部、６－１，６－２は認証データベース、７はＰＰＰ（ＰＰＰｏＥ）セッション、８はＨＴＴＰセッション、９－１はＮＩＣごとに設定されているＭＡＣアドレスを検出するＭＡＣアドレス検出部、９－２はＮＩＣごとに設定されているＭＡＣアドレスを検出するＭＡＣアドレス検出プラグイン（Ｐｌｕｇ－ｉｎ）、１０－１，１０－２，１０－３，１０－４は物理レイヤ、１１－１はユーザ端末側のＰＰＰレイヤ、１１－２はＢＡＳあるいはＢＳＮ側のＰＰＰレイヤ、１２－１はユーザ端末側のＨＴＴＰレイヤ、１２－２はＷｅｂサーバ側のＨＴＴＰレイヤ、１３－１，１３－２はＰＰＰｏＥレイヤ、１４－１，１４－２はＴＣＰ／ＩＰレイヤを示す。なお図示しないが、ユーザ端末１－１とＢＡＳ１－２のあいだにＡＴＵとＤＳＬＡＭが設置される。ユーザ端末１－１とＡＴＵはＥｔｈｅｒｎｅｔ接続、ＡＴＵとＤＳＬＡＭはＡＤＳＬ回線接続、ＤＳＬＡＭとＢＡＳ１－２はＡＴＭ専用線による接続が一般的である。

【００１６】実施形態例１（ＰＰＰｏＥクライアント、サーバがＭＡＣアドレスを認証に用いる場合）：図１の構成図において、ＰＰＰｏＥクライアント部２－１でＰＰＰｏＥサーバ部２－２に接続するとき、図３に示すように、ユーザは、ＰＰＰｏＥクライアント部２－１を起動し、ＰＰＰｏＥクライアント部２－１に対しＰＰＰｏＥサーバ部２－２への接続要求を行う。ＰＰＰｏＥサーバ部２－２はＰＰＰｏＥクライアント部２－１に認証要求を送る。ＰＰＰｏＥクライアント部２－１は、ＭＡＣアドレス検出部９－１によりユニックス（Ｕｎｉｘ）のｉｆｃｏｎｆｉｇコマンドやウィンドウズ（登録商標）

（Ｗｉｎｄｏｗｓ）のｉｐｃｏｆｉｎｇコマンドに該当する機能を用いて、図２に示すように、物理レイヤ１０－１から当該ユーザパソコンのＭＡＣアドレスを取得する。ＭＡＣアドレス検出部９－１は、ＰＰＰｏＥクライアント部２－１にＭＡＣアドレスを渡し、ＰＰＰｏＥクライアント部２－１は、ユーザが入力した「ユーザ＠ｒｅａｌｍ名」、「パスワード」、及び自動検出した「ＭＡＣアドレス」の認証情報をＰＰＰ（ＰＰＰｏＥ）フレームに格納し、ＰＰＰｏＥサーバ部２－２に送出する。

【００１７】ＰＰＰｏＥサーバ部２－２の認証データ抽出部４－２は、ＰＰＰｏＥクライアント部２－１から送られた認証情報から「ユーザ＠ｒｅａｌｍ名」、「パスワード」、「ＭＡＣアドレス」の認証データを取り出して、ユーザ認証部４－１が認証データを認証データベース６－１に送出し、照合する。認証データのすべてが一致した場合はユーザが認証（認証１）されたとみなし、ＰＰＰｏＥクライアント部２－１とＰＰＰｏＥサーバ部２－２の間でＰＰＰ（ＰＰＰｏＥ）セッション７を確立する。

【００１８】実施形態例２（ＨＴＴＰクライアント、サーバがＭＡＣアドレスを認証に用いる場合）：ＰＰＰｏＥクライアント部２－１は、ＰＰＰｏＥクライアント部２－１を起動し、ユーザが入力した「ユーザ＠ｒｅａｌｍ名」と「パスワード」をＰＰＰ（ＰＰＰｏＥ）フレームに格納し、ＰＰＰｏＥサーバ部２－２に送出する。ＰＰＰｏＥサーバ部２－２では従来方式どおり「ユーザ＠ｒｅａｌｍ名」と「パスワード」を用いて認証（認証１）を行い、ＰＰＰ（ＰＰＰｏＥ）セッション７を確立する。

【００１９】ＨＴＴＰクライアント部３－１は、ＰＰＰ（ＰＰＰｏＥ）セッション７上で、ＨＴＴＰセッション８を確立し、ＨＴＴＰクライアント部３－１とＨＴＴＰサーバ部３－２が通信を行う。ＨＴＴＰクライアント部３－１とＨＴＴＰサーバ部３－２間で認証が必要な場合が発生した場合、本発明では、以下のような認証を行う。

【００２０】図１で、ＨＴＴＰクライアント部３－１はＨＴＴＰサーバ部３－２に接続するとき、ユーザはＨＴＴＰクライアント部３－１に対しＨＴＴＰサーバ部３－２への接続要求を行う。図５に示すように、ＨＴＴＰサーバ部３－２はＨＴＴＰクライアント部３－１に認証要求を送る。ユーザはＨＴＴＰクライアント部３－１に対して、「ユーザ名」、「パスワード」を入力し、ＨＴＴＰクライアント部３－１はＭＡＣアドレス検出要求をし、図４に示すように、ＭＡＣアドレス検出プラグイン（Ｐｌｕｇ－ｉｎ）９－２により物理レイヤ１０－３から当該ユーザパソコンのＭＡＣアドレスを自動検出して取得する。ＭＡＣアドレス検出プラグイン（Ｐｌｕｇ－ｉｎ）９－２は、ＨＰＰＴクライアント部３－１にＭＡＣアドレスを渡し、ＨＴＴＰクライアント部３－１は、「ユーザ名」、「パスワード」、「ＭＡＣアドレス」の認証情報をＨＴＴＰフレームに格納し、ＨＴＴＰサーバ部３－２へ送出する。

【００２１】ＨＴＴＰサーバ部３－２の認証データ抽出部５－２は、ＨＴＴＰクライアント部３－１から送られた認証情報から「ユーザ名」、「パスワード」、「ＭＡＣアドレス」の認証データを取り出し、認証データを認証データベース６－２と照合する。認証データのすべてが一致した場合はユーザが認証（認証２）されたとみなし、ＨＴＴＰクライアント部３－１とＨＴＴＰサーバ部３－２間でＨＴＴＰセッション８を確立し、アクセス可能にして通信が行われる。

【００２２】実施形態例３（ＰＰＰｏＥ，ＨＴＴＰともにＭＡＣアドレスを認証に用いる場合）：上記、実施形態例１と実施形態例２を同時に行うことで、ＰＰＰｏＥによるＰＰＰ（ＰＰＰｏＥ）セッション確立時とＨＴＴＰによるセッション確立時にＭＡＣアドレスを用いた認証を行う。

【００２３】

【発明の効果】以上述べたように本発明によれば、ＮＩＣごとに一意であるＭＡＣアドレスを認証に用いることにより、ユーザ認証におけるセキュリティーを高め、なりすましを防ぐ効果がある。

【図面の簡単な説明】

【図１】本発明の実施形態例を示すシステム構成図である。

【図２】本発明の実施形態例に係るＰＰＰｏＥにおける認証機能のレイヤ構成図である。

【図３】本発明の実施形態例に係るＰＰＰｏＥにおける認証の処理フローを示すシーケンス図である。

【図４】本発明の実施形態例に係るＨＴＴＰにおける認証機能のレイヤ構成図である。

【図５】本発明の実施形態例に係るＨＴＴＰにおける認証の処理フローを示すシーケンス図である。

【図６】従来のユーザ認証システム構成の一例を示すブロック図である。

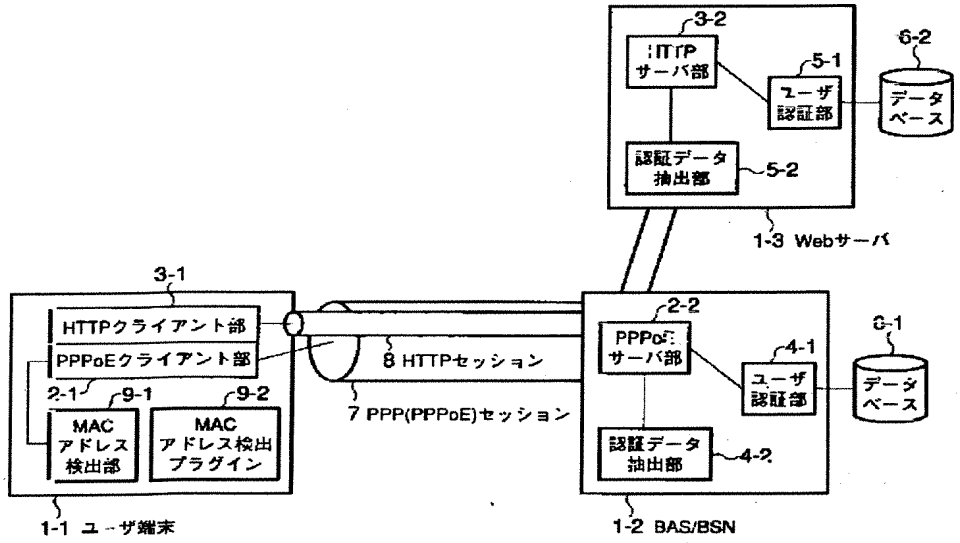
【図７】従来のユーザ認証方法における処理フローの一例を示すシーケンス図である。

【符号の説明】

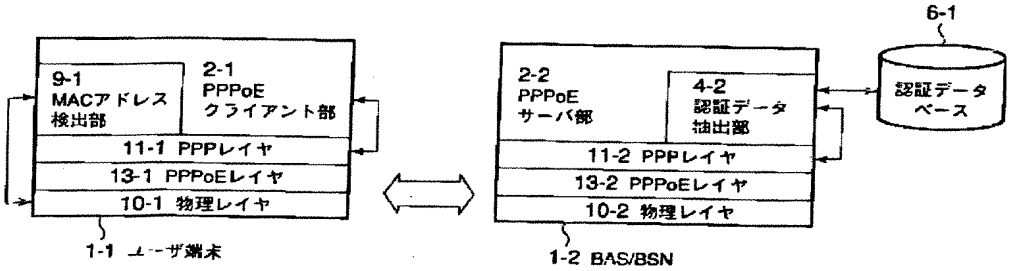
１－１　ユーザ端末
１－２　ＢＡＳあるいはＢＳＮ
１－３　Ｗｅｂサーバ
２－１　ＰＰＰｏＥクライアント部
２－２　ＰＰＰｏＥサーバ部
３－１　ＨＴＴＰクライアント部
３－２　ＨＴＴＰサーバ部
４－１　ＰＰＰにおけるユーザ認証部
４－２　ＰＰＰｏＥサーバ部における認証データ抽出部
５－１　ＨＴＴＰにおけるユーザ認証部
５－２　ＨＴＴＰサーバ部における認証データ抽出部

6－1，6－2　認証データベース
7　PPP（PPPoE）セッション
8　HTTPセッション
9－1　MACアドレス検出部
9－2　MACアドレス検出プラグイン（Plug－in）
10－1，10－2，10－3，10－4　物理レイヤ
11－1　ユーザ端末側のPPPレイヤ
11－2　BASあるいはBSN側のPPPレイヤ
12－1　ユーザ端末側のHTTPレイヤ
12－2　Webサーバ側のHTTPレイヤ
13－1，13－2　PPPoEレイヤ
14－1，14－2　TCP／IPレイヤ

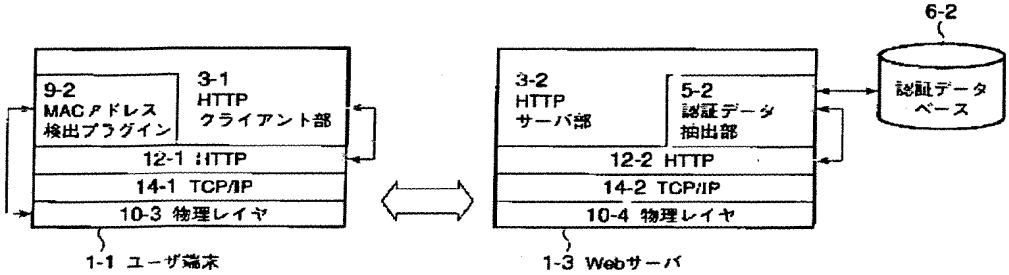
【図1】



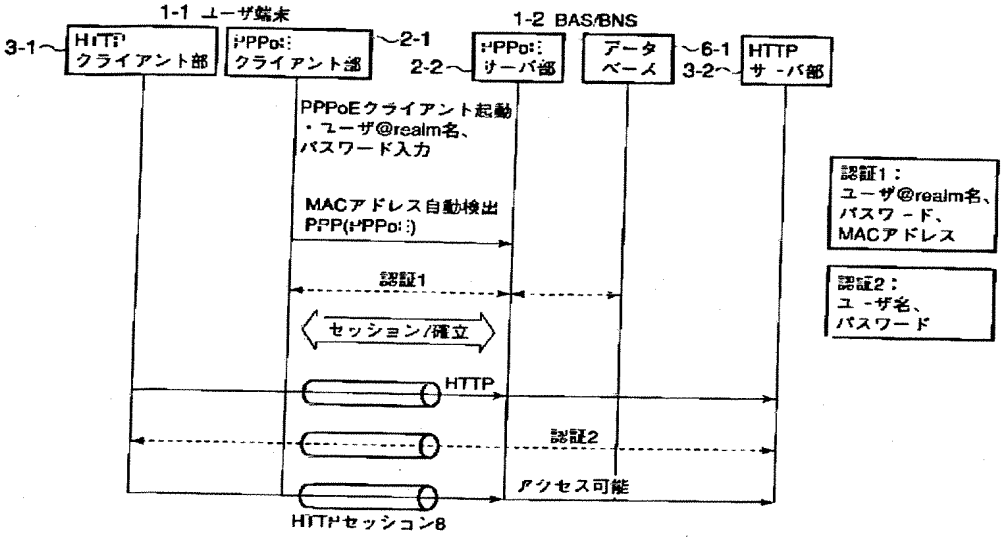
【図2】



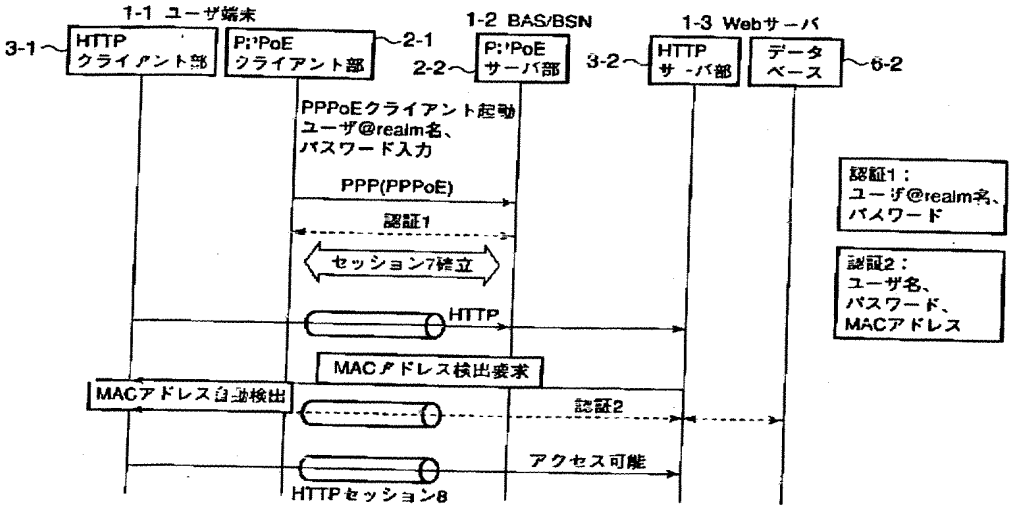
【図4】



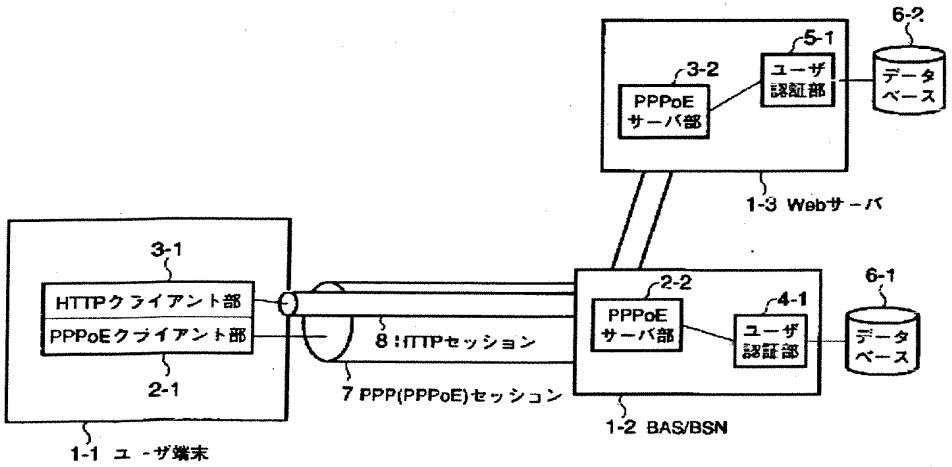
【図3】



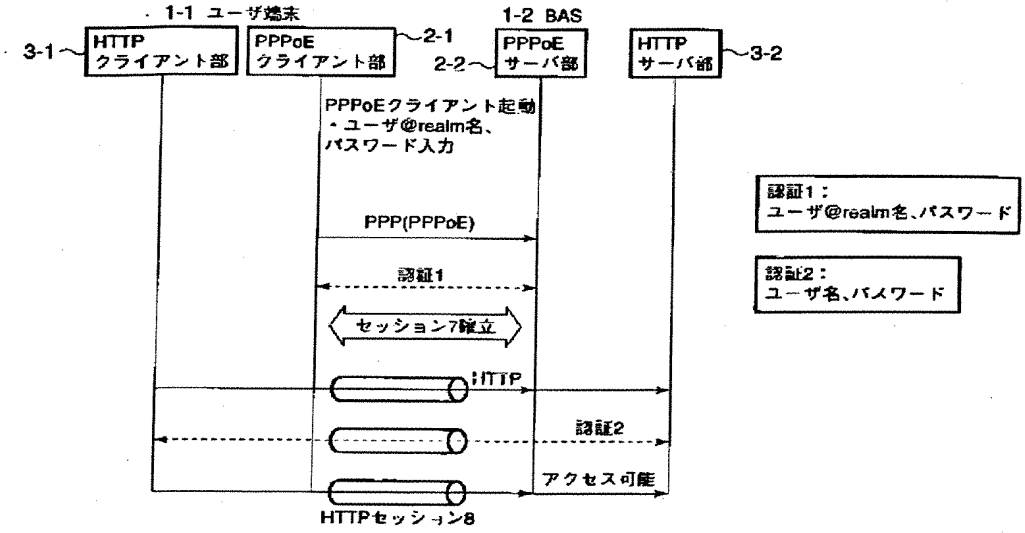
【図5】



【図6】



【図7】



フロントページの続き

(72)発明者　佐々木　将人
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

(72)発明者　渡瀬　順平
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B085 AE04 AE23 BG07
5J104 AA07 KA01 NA05 PA07